ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Preventing Jamming and Replay Attack in Wireless Applications

Pratibha S. Gaikwad, Prof. S. P. Pingat

PG Student, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, India

Assistant Professor, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, India

ABSTRACT: Wireless networks, are susceptible to a wide range of Denial-of-Service attacks which does not follow MAC protocol. Due to the open access and shared nature wireless communication systems are often vulnerable to the jamming attack where adversaries attempt to transmit radio interference to disrupt communication. Another simple denial-of-service attack is replay attack which is also easy to launch due to its principle based on two simple operations that is recording and resending massages. In order to detect and cope with this kind of Denial-Of- Service (DOS) style attack, many strategies have been developed. The traditional method spread spectrum techniques is use overcome the jamming attacks, which include frequency hopping and direct sequence spread spectrum. Anti-jamming techniques should support the device communication during the key establishment that requires devices have to share a secret key before start of the communication but it creates circular dependency. Therefore, research interest in wireless network has been growing since last few years.

In this paper, we proposed a integration of timestamp discrepancy and packet delivery ratio to validate a message and consequently to detect jamming attack. Our proposed timestamp scheme estimates the time where the message is transmitted, received and validated at receiver node. Replay attack detection and prevention is performed by using concept of packet delivery ratio and packet filtration. After detecting actual malicious node prevention is performed, in order to gain security in network. So to mitigate above attack solution is provided by using random key generation.

KEYWORDS: Jamming detection, Replay packet attack, Timestamp, Asymmetric key, Anti-jamming wireless communication.

I. INTRODUCTION

Wireless technologies have become increasingly popular in our day to day business and individuals lives. It enables one or more devices to communicate with each other without requiring cabling. The broadcast nature of wireless networks makes them particularly susceptible to the radio signal interference, which avoids the normal network communications. The jamming can disrupt the wireless transmission, reception and may occur either by means of interference or collision at the receiver side. Therefore it is primary concern from researcher point of view to detect different types of attacks in wireless networks. Normally Jamming attacks have been considered under an external threat model, but here we are considering jamming attacks under an internal threat model. Some possible strategies are given below.

1. Reactive jamming: An alternative approach to jamming wireless communication is to use a reactive strategy. Reactive jammers are aware of the target communication systems. They become quiet when the channel is idle, but start transmitting radio signals to undermine ongoing communication as soon as they sense activity on the wireless channel. This strategy targets the reception of a message and one advantage of a reactive jammer is that it is easy to launch but hard to detect [1].
2. Non-reactive jamming: Nonreactive jammers are not aware of any behavior of legitimate nodes and transmit the radio interference over the wireless channel following their own jamming strategies. Active jammers are usually effective because they keep the channel busy all the time [1].

Another simple and effective strategy for wireless DoS is the replay attack which locally heard data packets. These packets are then passed by another forwarding nodes resulting in increased levels of congestion and redundancy at each

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

forwarding nodes. A replay attacker performs this attack at anywhere and any time in the network. Many ideas have been proposed to prevent these attacks.

II. MOTIVATION

The first stage in defense is to understand and detect the types of jamming attacks. Importance of wireless network is tremendously increases from last few years due to its ubiquitous nature. The open nature of the wireless channel leaves it vulnerable to intentional or unintentional interference attacks, typically referred to as jamming. For radio signal transmissions, an important problem is denial of service, because a lot of important applications rely on wireless communication. It is important to detect and prevent network from denial-of-service attacks. Single measurement not enough to identify effectiveness of jamming attack. Security of wireless network is also reveal due to another type of attack called replay attack which very easy to launch and difficult to detect. As wireless communication is one of the basic needs of today's live, therefore it necessary to protect communication from such vulnerability. Objective of paper is to detect jamming and replay packet attack and prevent system from this attack.

III. RELATED WORK

Xu et al. [3], studied feasibility of launching and detecting different types of jamming attacks. In this paper they conclude that using carrier sensing time, packet sent ratio and packet delivery ratio individually, one is not able to classify the presence of a jamming attack. So paper improved detection technique by introducing concept of consistency check. They have proposed two enhanced detection algorithm: one is taking signal strength as a consistency check and other considering location information as consistency check. Consistency checking scheme improves detection performance. Frequency of the location advertisement is critical to which directly affects performance.

Ali et al. [4], present scheme for detection of jamming attacks in wireless adhoc networks. They proposed new method error distribution to detect jamming attack and use the scheme called correlation to measure association between two variables. Presented a new model based on the measure of correlation among error and correct reception time to identify presence of jamming attack in adhoc network. Main goal is to detect specific type of jamming attack. With the proposed method, able detect the presence of jamming attack with high degree of confidence. An advantage of proposed scheme is its simplicity and efficiency. If correlation relation is not linear then results are inaccurate.

Li et al. [6], studied intelligent jamming attacks in wireless sensor network which are easy to launch and hard to detect. Adversary controls probability of jamming and transmission range to cause maximum harm to the network. Jammer is detected at monitoring node by applying optimal detection test based on percentage of incurred collision.
In paper [7], presents scheme broadcast dynamic jamming mitigation using the combination of spread spectrum and binary key tree. Proposed method provides high performance.

Liu et al. [8], studied different anti-jamming technique such as frequency hopping and direct sequence spread spectrum. Paper presents novel, efficient and robust method called USD-FH (Uncoordinated seed disclosure frequency hopping). Scheme provide secret key in the existence of adversaries. Uncoordinated seed disclosure frequency hopping make use of a one-time pseudo random hopping pattern to broadcast each DH key establishment message and then reveal the seed of the pseudo random hopping pattern in an uncoordinated form before the actual message transmission. Proposed scheme advantages are robust and most efficient than previous approaches.

In paper [10], they considers a variant of the data packet rep-lay attack and these packets increases levels of congestion and interference enhance in large portions of the network. Adversary can either simply replay packet as it is or can modify packet header to make illusion of new packet. Presents detection and prevention technique COPS (for Copycat Online Prevention System). This technique uses combination of digital signature and bloom filters to deal with the attack. Proposed scheme consider only a percentage of packets is signed and load of verification is distributed along the nodes. Processing overhead is reduced by proposing attack mitigation using a combination of digital signatures and bloom filters. Advantages of this method, low resource consumption and processing overhead is reduced.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

IV. PROPOSED SYSTEM

In this paper, we provided an in-depth study on the impact of jamming and replay packet attacks in the wireless applications. It is very easy to launch jamming and replay attack but it is hard to detect. We design the system to achieve efficient and robust jamming and replay packet attack detection with prevention. Due to the shared nature and the open access to the wireless medium, jamming attacks have become common problem. The paper proposed concept of combined approach of timestamp and packet delivery ratio to detect jamming attack. Prevention is done by filtering the replay packet which is responsible for network jamming.

It also helps in detection and prevention attack like replay attack and blocking IP address of actual attacker in the network. Receiver node is responsible for detecting jamming and replay attack and prevention from actual attacker.

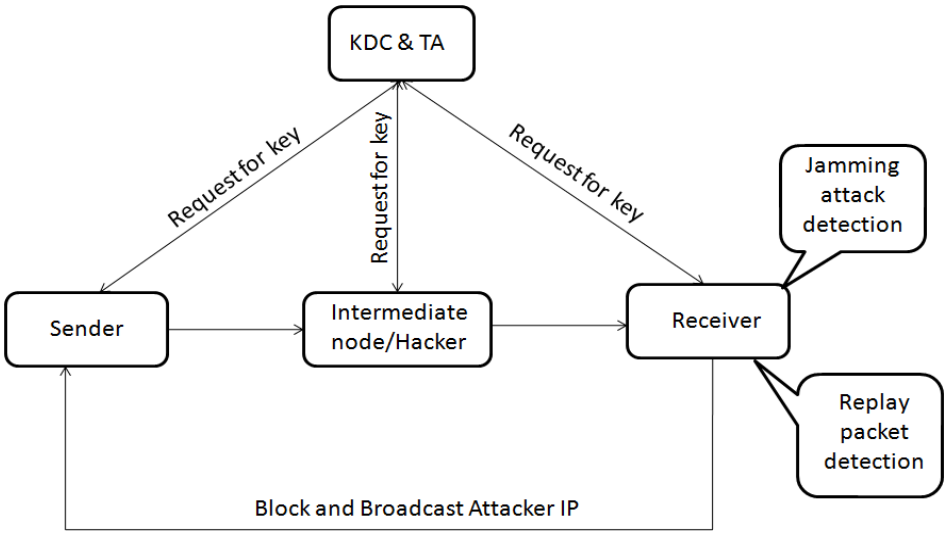

Fig 1: Proposed System Architecture.

V. ALGORITHM

Algorithm for jamming attack Detection:

```
At Sender:
For each packet
        {
                T1 = Calculate current time stamp for packet send;
                Send (Packet +T);
                Send (Packet +T1,H(T1));
        }
At Receiver:
{
        T2 = calculate time stamp when packet received.
        Calculate Tdiff;
        Tdiff = T2-T1;
        Threshold Thr = previously measured;
        If  (Tdiff >Thr)
        {
                if(PDR < 1)
                {
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

```
                Jamming attack occured with packet loss.
                }
                else
                {
                Jamming attack occured with no packet loss.
                }
        }
        else
        {
                Packet received normally.
        }

}.
```

VI. RESULT AND DISCUSSION

The below graph shown in fig2 is the no of packets vs time graph, which shows that the time required for the transmission of no of packet for normal transmission and with jamming transmission of packets. With jamming attack transmission packet requires more time for the transmission as the attacker may hold the packets during packet forwarding through intermediate node. In fig3 graph shows the no. of packet transmitted in normal and replay packets attack. Packet delivery ratio of replay packets is always greater than normal packet delivery ratio.

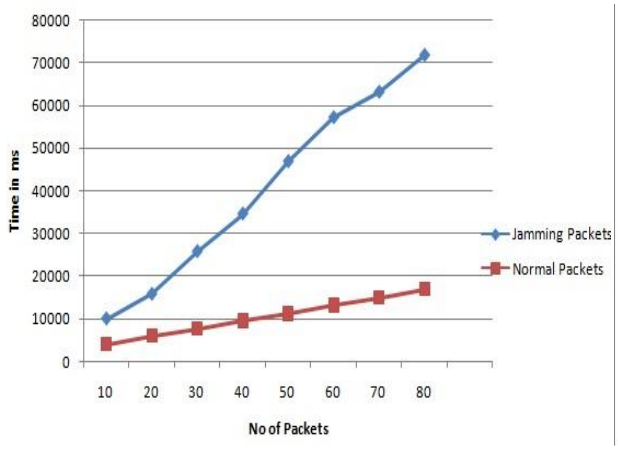

Fig2. No. of Packets vs. Time

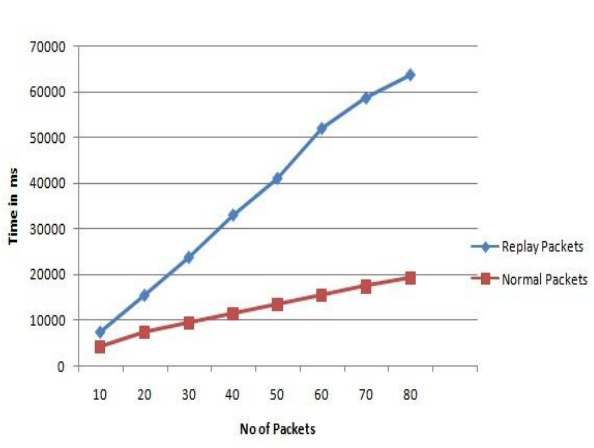

Fig3. No. of Packets vs. Time

VII. CONCLUSION AND FUTURE WORK

Proposed system gives idea about detection and prevention of jamming and replay packet attack. Detecting any type of attack is the first step in defeating it. In this paper we developed a novel, efficient and robust scheme to detect jamming attack. Detection of jamming attack and packet replay attack is done by scheme called timestamp and packet filtering. We found actual adversary and prevents such type of adversary and broadcast IP address of actual attacker in network to restore system to normal network operation.

The proposed algorithm provides efficient detection of jamming attack and replay attack. Proposed method maximizes the lifetime of entire network using prevention of attacks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

REFERENCES

[1] Zhuo Lu, Wenye Wang and Cliff Wang, "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless applications", IEEE ,August 2014
[2] S. Malladi, J. Alves-Foss, R. B. Heckendorn, "On Preventing Replay Attacks on Security Protocols", International Conference on Security and Management, 2002.
[3] Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", in Proc. ACM MobiHoc, Urbana-Champaign, IL, pp. 46-57, USA, 2005
[4] A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless adhoc networks using error distribution", IEEE ICC, Dresden, Germany, Jun.2009.
[5] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-ofservice attacks in CSMA/CA wireless networks", IEEE Trans, volume 3, pp. 347?358, Sep. 2008.
[6] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks", IEEE INFOCOM, pp. 1307-1315, May 2007
[7] An Liu, Peng Ning, Huaiyu Dai, Yao Liu "USD-FH: JammingresistantWireless Communication using Frequency Hopping with Uncoordinated Seed Disclosure", IEEE 2010
[8] Yao Liu, Peng Ning, Huaiyu Dai, An Liu, "Randomized Differential DSSS:Jamming-Resistant Wireless Broadcast Communication".
[9] Aldo Cassola, Tao Jin, Guevara Noubir, Bishal Thapa,"Efficient Spread Spectrum Communication without Pre-shared Secrets".
[10] Jerry T. Chiang, Yih-Chun Hu "Dynamic Jamming Mitigation for Wireless Broadcast Networks".
[11] Zi Feng, Jianxia Ning, Ioannis Broustis "Coping with Packet Replay Attacksin Wireless Networks".
[12] Ms. Pratibha S. Gaikwad and Prof. S. P. Pingat "Detection of attacks based on timestamp discrepancy", IJARCET, Volume 4 Issue 6, June 2015.